

## CLAIMS

1           1.       Method for verifying a signature, or respectively an authentication, by  
2 means of an asymmetric private-key and public-key cryptographic calculation process  
3 between a "*prover*" entity and a "*verifier*" entity, the prover entity performing  
4 cryptographic calculations with said private key in order to produce a signature  
5 calculation, or respectively an authentication value constituting a response value, and the  
6 verifier entity, based on this response value, performing cryptographic calculations with  
7 said public key in order to perform this signature verification, or respectively this  
8 authentication, the cryptographic calculation operations implementing the calculation of  
9 the modulo-n or large-number multiplications, characterized in that for a cryptographic  
10 calculation process using a public key comprising a public exponent  $e$  and a public  
11 modulo  $n$ , and a private key comprising a private exponent, it comprises the following  
12 steps"

- 13           - calculating at the level of said prover entity at least one prevalidation value;
- 14           - transmitting from the prover entity to the verifier entity at least said one
- 15 prevalidation value, this prevalidation value allowing the verifier entity to perform at
- 16 least one modular reduction without any division operation for this modular reduction.

1           2.       Method according to claim 1, characterized in that for a public exponent  
2  $e=2$ , the cryptographic calculation processing being based on a RABIN algorithm, said at  
3 least one prevalidation value comprises a unique value, which is the quotient  $Q$  of the  
4 square of said respective value of a signature or a response by said public modulo  $n$ ,  $Q =$   
5  $R^2/n$ , where  $R$  designates said respective value of a signature or a response to an  
6 authentication.

1           3.       Method according to claim 2, characterized in that after the reception by  
2 said entity of said respective value of a response to an authentication verification or a  
3 signature of a message ( $M$ ), and of said at least one prevalidation value comprising said  
4 quotient, this method comprises, at the level of said verifier entity, the following steps:

- calculating the difference ( $D_{AR}$ ,  $D_{SR}$ ) between the square of the response value  $R \cdot R$  and the product  $Q \cdot n$  of said quotient  $Q$  by said public modulo  $n$ , ( $D_{AR}$ ,  $D_{SR} = R \cdot R - Q \cdot n$ );
- verifying the equality of said difference with the value of a function of this response value, without any division operation by the modulo  $n$  operation.

4. Method according to claim 1, characterized in that for a public exponent  $e = 3$ , the cryptographic calculation process being based on an RSA algorithm, said at least one prevalidation value comprises:

- a first quotient  $Q_1$  of the square  $R \cdot R$  of said response value  $R$  by said public modulo  $n$ ;

- a second quotient  $Q_2$  of the product of said response value and the difference between the square  $R \cdot R$  of this response value and the product of said first quotient  $Q_1$  and the public modulo  $n$ , by said public modulo  $n$ ,  $Q_2 = R \cdot (R \cdot R - Q_1 \cdot n) / n$ .

5. Method according to claim 4, characterized in that after the reception of said response value R and said at least one prevalidation value comprising said first and second quotients  $Q_1$  and  $Q_2$ , said method comprises, at the level of said verifier entity, the following steps:

- calculating the difference ( $D_{ARSA}, D_{SRSA}$ ) between the product of said response value  $R$  and the difference between the square  $R*R$  of this response value and the product of said first quotient  $Q_1$  and the public modulo  $n$ , and the product of said second quotient  $Q_2$  and said public modulo  $n$  ( $D_{ARSA}, D_{SRSA}$ ) =  $R*(R*R - Q_1*n) - Q_2*n$ ;

- verifying the equality of this difference with the value of a function of said response value, without any division operation by modulo n operation.

6. Method according to claim 3 or 5, characterized in that for an operation for verifying a signature of a message (M), said function comprising a standardized public function  $f(M)$  of this message M, it comprises the following steps:

